2

AIR COMMAND AND STAFF COLLEGE

STUDENT REPORT

SECURITY HANDBOOK FOR SMALL COMPUTER USERS

MAJOR JANET B. WITHROW 85-2910

"insights into tomorrow"

DISCLAIMER

The views and conclusions expressed in this document are those of the author. They are not intended and should not be thought to represent official ideas, attitudes, or policies of any agency of the United States Government. The author has not had special access to official information or ideas and has employed only open-source material available to any writer on this subject.

This document is the property of the United States Government. It is available for distribution to the general public. A loan copy of the document may be obtained from the Air University Interlibrary Loan Service (AUL/LDEX, Maxwell AFB, Alabama, 36112) or the Defense Technical Information Center. Request must include the author's name and complete title of the study.

This document may be reproduced for use in other research reports or educational pursuits contingent upon the following stipulations:

-- Reproduction rights do not extend to any copyrighted material that may be contained in the research report.

-- All reproduced copies must contain the following credit line: "Reprinted by permission of the Air Command and Staff College."

-- All reproduced copies must contain the name(s) of the report's author(s).

-- If format modification is necessary to better serve the user's needs, adjustments may be made to this report--this authorization does not extend to copyrighted information or material. The following statement must accompany the modified document: "Adapted from Air Command and Staff Research Report __(number)__ entitled __(title)__ by __(author)__."

-- This notice must be included with any reproduced or adapted portions of this document.

REPORT NUMBER 85-2910

TITLE SECURITY HANDBOOK FOR SMALL COMPUTER USERS

AUTHOR(S) MAJOR JANET B. WITHROW, USAF

FACULTY ADVISOR MAJOR CHARLES E. ZIMMER JR, ACSC/EDCM

SPONSOR GM-13 PAUL A. TRAPP, AFTPC/CK

Submitted to the faculty in partial fulfillment of
requirements for graduation.

AIR COMMAND AND STAFF COLLEGE
AIR UNIVERSITY
MAXWELL AFB, AL 36112

AD A 157 091

REPORT DOCUMENTATION PAGE

1a. REPORT SECURITY CLASSIFICATION
UNCLASSIFIED

1b. RESTRICTIVE MARKINGS

2a. SECURITY CLASSIFICATION AUTHORITY

3. DISTRIBUTION/AVAILABILITY OF REPORT

2b. DECLASSIFICATION/DOWNGRADING SCHEDULE

4. PERFORMING ORGANIZATION REPORT NUMBER(S)
85-2910

5. MONITORING ORGANIZATION REPORT NUMBER(S)

6a. NAME OF PERFORMING ORGANIZATION
ACSC/EDCC

6b. OFFICE SYMBOL *(If applicable)*

7a. NAME OF MONITORING ORGANIZATION

6c. ADDRESS *(City, State and ZIP Code)*
Maxwell AFB AL 36112

7b. ADDRESS *(City, State and ZIP Code)*

8a. NAME OF FUNDING/SPONSORING ORGANIZATION

8b. OFFICE SYMBOL *(If applicable)*

9. PROCUREMENT INSTRUMENT IDENTIFICATION NUMBER

8c. ADDRESS *(City, State and ZIP Code)*

10. SOURCE OF FUNDING NOS.

PROGRAM ELEMENT NO.	PROJECT NO.	TASK NO.	WORK UNIT NO.

11. TITLE *(Include Security Classification)*
SECURITY HANDBOOK FOR SMALL COMPUTER USERS (U)

12. PERSONAL AUTHOR(S)
Withrow, Janet B., Major, USAF

13a. TYPE OF REPORT

13b. TIME COVERED
FROM ________ TO ________

14. DATE OF REPORT *(Yr., Mo., Day)*
1985 April

15. PAGE COUNT
76

16. SUPPLEMENTARY NOTATION

17. COSATI CODES

FIELD	GROUP	SUB. GR.

18. SUBJECT TERMS *(Continue on reverse if necessary and identify by block number)*

19. ABSTRACT *(Continue on reverse if necessary and identify by block number)*

The fielding of large numbers of small computers throughout the Air Force has precipitated the need for a small computer security handbook. Unlike traditional large computer systems, small computers are being used extensively by functional users in non-controlled environments. As a result, users of these small systems must be made aware of their security responsibilities in safeguarding the small computer and the data it processes. This handbook highlights small computer security issues and makes users aware of their security responsibilities in using a small computer. It supersedes A Small Computer Security Handbook published by the Air Force Small Computer/Office Automation Service Organization in 1983.

20. DISTRIBUTION/AVAILABILITY OF ABSTRACT
UNCLASSIFIED/UNLIMITED □ SAME AS RPT. □ DTIC USERS □

21. ABSTRACT SECURITY CLASSIFICATION
UNCLASSIFIED

22a. NAME OF RESPONSIBLE INDIVIDUAL
ACSC/EDCC Maxwell AFB AL 36112

22b. TELEPHONE NUMBER *(Include Area Code)*
(205) 293-2483

22c. OFFICE SYMBOL

PREFACE

The need for a small computer security handbook has been precipitated by the fielding of large numbers of small computers throughout the Air Force. The Tactical Air Force's contract with Virginia Communications Association for Cromemco systems along with the two Air Force/Navy standard contracts with Zenith Data Systems for the Zenith Z-100 and the TEMPEST Z-150 systems have been primary drivers in this large scale introduction of small computers. With small computer systems now located in functional users' offices, responsibility for computer security has shifted from the traditional data automators to the functional users. In addition, with the contract award for a standard TEMPEST small computer system, the safeguarding of classified computer data is now a major security issue.

Small computers differ from the traditional large systems in two respects. They are no longer operated solely by data automators, but are in the hands of functional users who are not trained in computer systems technology. In addition, these systems are no longer located within the confines of a controlled computer facility, but located throughout functional user areas. Thus, accessibility to these small systems is a major concern. We must now deal with the resulting security implications of these two differences. Users of these small computers must be made aware of their security responsibilities in safeguarding these systems. The Air Force recognizes the security implications in fielding these small systems and the importance of user involvement. The management and use of small computers has now become an item of interest with the Air Force Inspector General (26:--).

This handbook attempts to highlight security issues for small computer systems and make users aware of their computer security responsibilities. It identifies applicable Air Force security directives and applies the requirements of those directives to small computer technology. It supersedes A Small Computer Security Handbook published by the Air Force Small Computer/Office Automation Service Organization (AFSCOASO) in 1983. Its actual development responds to tasking from the Director of Integration and Technology, Assistant Chief of Staff, Information Systems, Headquarters United States Air Force (HQ USAF/SIT) (21:--; 22:--).

ABOUT THE AUTHOR

Major Janet B. Withrow is an information systems officer, AFSC 51XX. Prior to attending Air Command and Staff College in residence, she spent 2 1/2 years at the Air Staff in the Office of Information Technology, Deputy Chief of Staff, Plans and Operations (HQ USAF/XC-I). During that period, she participated in the effort to field small computers throughout the Air Force by working on the projects for the Air Force standard unclassified and TEMPEST small computers. She was a key player in introducing small computer technology within the operations staff to include a TEMPEST prototype small computer system. She developed the security plan and accompanying security procedures for the use of this prototype system in processing sensitive and classified information.

Major Withrow has a bachelor of science degree in chemistry from St. Mary's College of Notre Dame and a master of science degree in computer systems from the Air Force Institute of Technology. She will graduate in June from the Air Command and Staff College.

TABLE OF CONTENTS

APPENDICES:

CHAPTER 1

"What is this handbook?"

Introduction

As a user of a small computer system you are responsible for its security (6:30). The purpose of this handbook is to make you aware of small computer security issues and to suggest approaches to dealing with these security problems.

This handbook is for those who use Air Force small computer systems, regardless of technical background in either computer or security issues. AFR 300-3 provides the Air Force definition of a small computer. For purposes of this handbook, a small computer or small computer system includes the entire suite of hardware (microprocessor, memory, disk drives, keyboard, video display, printer, etc.), software (operating system, word processor, user-developed applications programs, etc), and user's data (24:2-2). These guidelines apply to small computer sytems in a single-user, standalone configuration. Thus, this handbook applies to small computer systems to include deployable systems (e.g., TAF's Cromemco), portable systems (e.g., MAC's Osbornes), and word processing systems (e.g., CPTs and Wang systems) (6:2). This security guidance applies to the Air Force standard small computer systems (the Zenith Z-100 and the TEMPEST Zenith Z-150) in standalone configuration as well as the Sperry PC small computer system, an IBM PC, or other systems in a single-user, standalone configuration. In Chapter 6, we will look beyond a standalone configuration and briefly touch upon security considerations when your system is configured to interface with another system via some type of communications link.

A number of security directives serve as the sources of Air Force security requirements. This handbook attempts to consolidate the requirements of these directives. In particular, when a specific directive is cited, you will know the following guidance provides an acceptable alternative for implementing the policy of that directive. For example, this handbook provides procedures for declassifying a small computer system, a process required by both AFR 205-1 and AFR 205-16. The procedure this handbook recommends meets the Air Force requirements for declassifying a small computer system. In addition, you should be aware this handbook does not consolidate requirements for processing either Single Integrated Operational Plan - Extremely Sensitive Information (SIOP-ESI) data or Sensitive Compartmentalized Information (SCI) and other foreign intelligence data. If you process either of these data types, check on the additional processing requirements before using the system.

You do not have to be a small computer expert to read this handbook. However, you should be familiar with basic small computer terminology such as operating system, floppy diskette, or random access memory. Recommend you become familiar with the small computer system by first reading either the user's manual or the operations guide that comes with the system.

From a security standpoint, you should be aware of AFR 300-3, Management of Small Computers, AFR 205-16, Automatic Data Processing (ADP) Security Policy, Procedures, and Responsibilities, and, of course, AFR 205-1, Information Security Program. If you do not have these three regulations in your office library, be sure to add them. You'll be needing them from time to time in maintaining security on your small computer system.

Roadmap

We will be looking at securing a small computer system for its entire life cycle. We'll look at small computer security risks from the perspectives of hardware, software, and data and consider a variety of security measures to reduce these risks, such as physical security and administrative security (6:16). First we'll define some terms and identify pertinent regulations, responsible organizations, and individual key players in Chapter 2. In the next three chapters, we'll explore security considerations before the system arrives (Chapter 3), once the system is installed (Chapter 4), and when it is in use (Chapter 5). We will also briefly discuss security implications when interfacing the system to an external source (Chapter 6). We've provided a number of appendices to help in maintaining the security of a small computer system. The appendices include sample sensitivity markings as well as a series of sample logs you'll be using. Appendix F briefly summarizes the contents of Chapters 3 through 5 by providing a general purpose security checklist for a small computer system.

Before looking at specific security issues, let's first define some terms and identify the pertinent regulations and key players in small computer security.

CHAPTER 2

"Before we begin . . ."

Introduction

This handbook will be more useful if we first develop a foundation from which to work. To do this we must first define the security terms we'll be using throughout this handbook, identify applicable security directives, and identify key organizations and individual players in small computer security matters.

Definitions

This handbook does not attempt to redefine terminology. Definitions for most small computer terms can be found in AFR 300-3, attachment 1. Computer security terms are defined in AFR 205-16, attachment 3. Some of the key terms used in this handbook are as follows:

Criticality - a measure of the "value" of the small computer system in supporting the mission and in protecting human life (25:—).

Declassification - a procedure performed on small computer hardware and supplies to remove all traces of classified information. No residual effects of classified material exist on the hardware or supplies (26:—).

Functional area - an organizational class using the small computer for a specific set of needs (26:—). For example, a flying squadron can be considered a functional area.

Life cycle - the entire life of a small computer system from its conceptual stage throughout its operational life (6:27).

Mode of operation - the manner of operating the small computer system to process, store, use, or produce sensitive or classified material (6:9).

Personal data - any item of information about an individual that is not a matter of public record and is usually considered to be personal to the individual (5:3). Personal information includes data covered under the Privacy Act of 1974. It includes legal, medical and financial information. It is often referred to as sensitive data to distinguish it from classified data (25:—).

Risk - a possibility that an incident will occur when a threat has a corresponding vulnerability (6:35).

Sensitivity - a measure of the "value" of the data. Sensitivity expands the concept of classified information to include classified data, personal data, "For Official Use Only" data, and other information that requires some degree of protection (25:—).

System sensitivity level - the highest level at which sensitive software or data is has been processed, stored, used, or produced on the system since the system was last declassified (26:—).

TEMPEST - a term used in referring to investigacions and studies of compromising emanations. Small computer hardware may generate compromising emanations. These emanations propogate through space, over telephone lines, through water pipes, and through other conductors of electricity (8:5-1). TEMPEST small computers refer to systems that do not emit electromagnetic radiation outside a given radius (2:930).

Threat - any force or phenomenon that could degrade the availability, integrity, or confidentiality of a small computer resource, system, or network (6:35).

Vulnerability - a weakness that may be exploited by a threat to cause harm to small computer resources (6:35).

Pertinent Regulations

The two primary regulations are:

AFR 205-1, Information Security Program; and
AFR 205-16, Automatic Data Processing (ADP) Security Policy, Procedures, and Responsibilities.

A complete list of security references can be found in AFR 205-16, attachment 1. AFR 205-16 serves as the main directive for this handbook since it implements AFR 205-1 for automated systems. Other regulations of interest are as follows:

If you process SCI or other foreign intelligence data, Defense Intelligence Agency Manual (DIAM 50-4) and USAF Intelligence (USAFINTWEL) 201-1 apply (6:2).

If you process SIOP-ESI data, AFR 205-25 applies (6:2).

You should also be aware of a new regulation to be published soon, AFR 700-10, Information Systems Security. This regulation establishes policies, assigns responsibilities, and provides guidance in planning information systems security and developing information systems security plans (19:1).

Responsible Organizations

A detailed listing of all organizations responsible for computer security can be found in AFR 205-16. The following is a listing of those organizations you especially need to know:

Air Force Computer Security Program Office (AFCSPO) - Air Force OPR for the technical implementation of HQ USAF developed computer security policy (6:8).

Air Force Office of Security Police (AFOSP) - Air Force Office of Collateral Responsibility for personnel, information, industrial, and physical security matters (6:3).

Air Force Small Computer/Office Automation Service Organization (AFSCOASO) - provides Air Force-wide small computer support services (10:3).

Director of Integration and Technology, Headquarters US Air Force (HQ USAF/SIT) - Air Force Office of Primary Responsibility (OPR) for computer security policy (6:3).

Headquarters Electronic Security Command (HQ ESC) - performs TEMPEST and communications security functions (6:8).

MAJCOM Small Computer Technical Center (SCTC) - central point of contact within a MAJCOM for small computer matters (10:3).

Some Individual Key Players

The following is a list of a few individual key players in small computer security. The list is far from complete. Look at AFR 205-16 for a comprehensive discussion.

Designated Approval Authority (DAA) - MAJCOM or Separate Operating Agency (SOA) commander or designated representative responsible for managing the MAJCOM/SOA security program. The DAA must approve the use of computer systems to process sensitive and classified information or for critical processing (6:4-5).

Equipment Control Officer (ECO) - person responsible for the Automatic Data Processing Equipment (ADPE) inventory at an installation. He or she is responsible for periodically performing physical inventory to verify the identity and location of the computer systems (7:5-1).

Equipment Custodian - designated by the ECO, the person responsible for the hardware inventory of a local area (e.g., the inventory of the small computer systems in an office) (7:5-1). Though not specifically required by regulation, this person should also maintain a current inventory of all software used on the small computer systems and monitor the backup of all software and data (26:--).

Functional area manager - the individual responsible for the overall computer operation within his or her functional area. He or she performs the same duties as the Automatic Data Processing Facility (ADPF) manager (see AFR 205-16) (6:6).

Information Systems Security Officer (ISSO) - functional area manager's "right arm man" for directing the computer security program (6:3).

Local TEMPEST officer - individual who provides guidance and assistance in TEMPEST matters (8:5-2).

Terminal Area Security Officer (TASO) - Appointed by the functional area manager, this person directs the computer security program within a local area (e.g., an office). He or she is the person to talk to if there are any questions about small computer security. He or she is also the person to contact if small computer security problems or incidents arise (6:5-6). Note there can be more than one TASO in an office. If, in an office, there are terminals connected to a another computer system, there will be a TASO for those terminals. There are also TASOs designated for standard Automatic Data Processing Systems (ADPSs). Don't get these other TASOs confused with the TASO responsible for the small computer systems (26:--).

Summary

Hopefully we have provided useful information to prepare you for reading the rest of this handbook. We've defined some terms, pointed out key regulations and responsible agencies, and looked at some individual key players you should know. We are now ready to take a look at security issues throughout the life cycle of a small computer system.

CHAPTER 3

"I need a small computer. Now what?"

Introduction

Having defined some terms and identified some key players, we can now begin looking at small computer security issues. We will lay the groundwork for the material in Chapters 3 through 5 by first introducing the concept of life cycle management and discussing how it applies to small computer security. We will then take a look at your responsibilities in planning for a small computer system.

Life Cycle Management

AFRs 300-12 and 300-15 discuss five phases in the life cycle of a computer system: conceptual, definition, development, test, and operation (6:27). Security has a role in each of these phases. AFR 205-16, attachment 6, details the actions to be taken in each of these phases to successfully ensure adequate security during a computer's life cycle. We shall look at a small computer's life cycle from a less detailed perspective. In these next three chapters we'll consider security before the system arrives, once it gets into the office, and when the system is actually in use.

In looking at the planning phase, that time before the system arrives, there are numerous security related activities in which you are involved. Since security measures are designed to reduce security risks, it is important these measures are addressed up front and included in the overall design of the small computer system. Without minimizing the importance of your involvement in many planning functions (see AFR 205-16, attachment 6 for details), we will concentrate on two vital areas that require your full participation while planning for a small computer system: the risk analysis and contingency planning.

The Risk Analysis

The risk analysis is a formal document written to describe the analysis performed to assess the threats to and vulnerabilities of the small computer system and evaluate possible measures to reduce the associated security risks (6:34). Since a detailed discussion of the risk analysis is provided in attachment 7 of AFR 205-16, we will not go into great detail here. We will, however, discuss your primary functions in the risk analysis.

In performing the risk analysis, there are two points to remember. First, you are a member of a risk analysis team. Other members of the team may include the ISSO, information systems (SI) personnel, security police, the fire department, base safety, the civil engineers, or others, as needed (6:37-38). Secondly, though a large portion of the risk analysis work is done during the planning phase of the system, it is never complete since small computer security risks must be continually evaluated throughout the system's life cycle (6:32-33). Your involvement in the risk analysis will vary depending on the life cycle phase of the system; however, your primary role in the risk analysis takes place during the system's planning phase.

Your involvement during the planning phase consists of four activities. They are as follows:

Step 1. Determine the type of data the small computer system will be processing;
Step 2. Determine the sensitivity of the data and applications to be processed;
Step 3. Determine the criticality of the small computer system; and,
Step 4. Consider various alternatives to reduce the risks and make trade-offs by evaluating risk reduction versus cost.

The first three steps will be your responsibility since only you, as the functional user of the system, can make those determinations. You will be working closely with your other key players in performing the fourth step (6:41-47).

Let's first look at step 1, determining the type of data to be processed. In considering the type of data, you need to look at not only the data you will process, but also any applications programs you will be using to process that data. You need to consider the classified level of the data and applications programs (i.e. confidential, secret, etc.) and to decide if any personal data will be processed. Don't consider only your immediate needs. Think about the next five years.

You next step is to determine the sensitivity of the data you plan to process. There are three sensitivity levels:

ADP-I: critical-sensitive,
ADP-II: noncritical-sensitive; and
ADP-III: nonsensitive.

The jargon is somewhat confusing, but we'll try to sort out what you must do without getting confused with terminology. In this step, you simply need to associate your findings from Step 1 with a sensitivity level. If you process top secret information the sensitivity level is ADP-I. If you process secret data, confidential data, or personal data, the sensitivity level is ADP-II. Anything less than that already mentioned is a sensitivity level of ADP-III. In addition, the sensitivity level is always that of the most sensitive data you will process (6:28). Recommend you look at Figure A6-1 of AFR 205-16 for more details.

You are required to determine the criticality of the system in Step 3. There are three criticality levels as follows:

ADP-I: highly-critical;
ADP-II: critical; and
ADP-III: non-critical.

This terminology is confusing since it is so similar to sensitivity terminology. However, don't let this terminology complicate your task. To determine the criticality of the system, you must decide upon the impact in either performing the mission or the risk to human life if an application cannot be performed or its input or output data is unreliable. If the impact to mission performance is grave or gravely jeopardizes human life, the criticality is ADP-I. If the impact to the mission is serious, the criticality is ADP-II. Anything less than that already mentioned is a criticality of ADP-III. For example, if the data base for a loadplanning applications program is inaccurate and you cannot load the aircraft without using that data base, you cannot perform the mission. In that case, the criticality of the small computer system is ADP-I. If the word processing package for handling routine administration is not working correctly, the criticality is probably ADP-III. Lastly, the criticality level of the system is the highest criticality level of any application performed (6:29). If the system has both ADP-I and ADP-III applications, the criticality of the system is ADP-I. Recommend you look at Figure A6-2 of AFR 205-16 for specific details.

The fourth step consists of evaluating various security measure alternatives and selecting the most appropriate for the system by considering risk reduction and cost trade-offs. This last step really has three parts:

Part 1: Assess the vulnerabilities of and threats to the small computer system;
Part 2: Apply alternative security measures to reduce the associated risks; and
Part 3: Perform a cost trade-off evaluating risk reduction versus cost (6:42-45).

This step appears to be very time consuming and cumbersome; however, it can be done quickly and simply. The basic vulnerabilities of and threats to a small computer system are already known. Chapter 4 presents a discussion of these vulnerabilities and threats and presents possible measures to reduce the associated risks (Parts 1 and 2). All you must do is present a brief rationale of the selected security alternatives (Part 3). Attachment 7 of AFR 205-16 suggests using one of several matrix formats (6:40-46). Remember to keep it brief and concise (6:34). Also remember that you, as the functional user, will not be doing this step alone. Work with the other players on the risk analysis team. The ISSO can be of particular assistance in this step (6:37-38).

There are numerous other phases to the risk analysis. If you are on the risk analysis team for the small computer system, you'll be involved in much more than the steps mentioned above. However, the four steps mentioned will be your key activities while planning for the small computer system.

Before closing this discussion on the risk analysis, let's reiterate one last point. The level of effort in conducting a risk analysis should be commensurate with the security threat to that system. A risk analysis for the WWMCCS computer system would be a large scale effort due to the complexity of the security threat; however, a risk analysis for a standalone small computer system should be a short and simple procedure. The risk analysis merely needs to document the security measures you plan to take to reduce security risks to the system. Use the format suggested in attachment 7 of AFR 205-16 for documenting the risk analysis.

Contingency Planning

The risk analysis serves as a tool for selecting security measures to protect the small computer system. A closely related activity is developing measures to protect your functional area from unexpected small computer losses. This vital step is known as contingency planning. A contingency plan is simply a set of procedures for recovering from losses of either software or data or small computer processing capability (24:5-20). It is designed to provide a reasonable continuity of operations should events occur which prevent normal small computer operations (16:5). Its importance cannot be overstated. In fact, AFR 205-16 requires a contingency plan for all critical (ADP-I and ADP-II) systems. Though not required by regulation, you should not overlook developing this plan eventhough the system is only "noncritical". (See Step 3 in the risk analysis discussion above.) Contingency procedures should be established for every small computer system.

There are two aspects that must be addressed in contingency planning. You must develop procedures for recovering from software or data losses and from losses in processing capability. Let's first look at planning for recovering from software or data losses. You must develop a workable plan enabling you to recover from intentional or unintentional losses. Developing a set of backup procedures is the primary way to deal with this potential problem (24:5-22). Several considerations need to be addressed in selecting a backup procedure: the value of the software and data in terms of both sensitivity and timeliness; the various methods available for backing up the data; and the location for storing the backup media. We'll not go into further detail here since backup procedures are discussed in Chapter 5; however, you must consider this procedure now, before the system arrives in your office.

You must also address potential loss of processing capability in the contingency plan. This portion of the plan is often called a contingency operations plan (24:5-22). Its purpose is to provide you a set of alternative methods for processing the data when the small computer system is not operational. There are two general requirements for the continuity operations plan:

1. The plan must include procedures for processing functions of differing criticality levels.
2. The plan must consist of a ranked order set of alternative procedures.

Let's look at the first requirement. You determined the criticality of the functions the system performs in conducting the risk analysis. (See Step 3 of the risk analysis discussion above.) We need to look again at the criticalities of these functions since the criticality will directly impact what alternatives will satisfy the processing requirement. If the system processes highly-critical (ADP-I), critical (ADP-II), and noncritical (ADP-III) functions, the contingency operations plan, should address three sets of alternative processing procedures for the three criticality levels. Let's give an example. Your small computer performs two functions - flight planning and suspense tracking. Flight planning has a criticality of ADP-I; suspense tracking is ADP-III. When the system is nonoperational, you still must accomplish the flight planning function. Your contingency operations plan may specify you use the system in the next office. However, automated suspense tracking is not a critical function, so reverting to a manual tracking mode is an acceptable alternative for the contingency operations plan. As this example shows, you have developed different alternative processing procedures because the criticality of the functions are different.

The contingency operations plan must also include a series of alternative processing procedures to deal with various threats to the processing capability of the system. For example, to deal with a hardware failure, the contingency operations plan may call for you to simply use the small computer system next door. However, if you live in a high risk area for tornadoes, you need another processing alternative to deal with that threat since the small computer next door may also be nonoperational if a tornado strikes the building. You must consider the various threats to the system in developing a rank ordered set of alternatives. Chapter 4 discusses the human and environmental threats to the small computer. Recommend you take a look at that chapter in developing alternative processing plans for your system.

Two last points about contingency operations plans. First, you may decide a second small computer system is the primary alternative for providing a contingency processing capability. If that is the case, you need to ensure this requirement is included as part of the overall system requirement. Second, you may need to develop written agreements with other functional areas if they are part of the contingency processing support. These written agreements can become very important when the small computer becomes nonoperational.

To summarize contingency planning, let's reiterate its importance. When you are planning for a small computer system, developing these plans may seem very bothersome, but these plans become very important once the system arrives and you have become dependent upon its processing capabilities to perform the mission. Contingency planning is mandatory for small computer systems of criticality levels ADP-I (highly critical) and ADP-II (critical). We highly recommend contingency planning for non-critical (ADP-III) small computer systems as well. You may find that a non-critical (ADP-III) small computer system has become a critical asset over time.

Summary

In this chapter we have discussed your involvement in planning for the security of a small computer system. We did not discuss all your activities. A full description is provided in attachment 7 of AFR 205-16. We did discuss two primary planning steps: the risk analysis and contingency planning. We will now leave the planning phase of a small computer's life cycle and take a look at the operational phase of a small computer system.

CHAPTER 4

"It's installed. What must I worry about now?"

Introduction

As mentioned in an earlier chapter, small computer security is designed to reduce risk by countering threats and vulnerabilities to a small computer system. Keeping these points in mind, we will now look at various vulnerabilities and threats to the small computer system once it arrives in the office.

Before we begin, let's limit our area of concern. We are concerned with the small computer system - its hardware, software, and data. AFR 205-16 specifically applies to these aspects of the system. We will not be detailing security procedures for handling small computer hardcopy (e.g., printer or plotter output) since security requirements for treating documentation are clearly defined in AFR 205-1 (9:--). We assume you are familiar with the security requirements of that regulation.

Let's briefly explain the layout of this chapter. We will be discussing security measures in terms of vulnerabilities and threats to the small computer system. There are two vulnerabilities inherent in today's small computer: its physical accessibility and the limited security mechanisms available in its hardware and software (24:2). In addition to these vulnerabilities, the security risk of a small computer is compounded by a series of threats. Threats are of two types: human (both intentional and unintentional) and environmental (17:--). In the remainder of this chapter we'll be identifying security risks in terms of the system's hardware, software, and data. You'll see that vulnerabilities and threats go hand-in-hand as we identify risks in terms of security threats and offer security measures to reduce the risk. Once we've covered those aspects, we'll take a look at several other related small computer security issues.

Protecting the Hardware

In the following discussion we will consider hardware to include the small computer itself and all its associated peripheral equipment. Such items as the video display, the keyboard, external disk drives, printers, and plotters are included.

Intentional human threats. Intentional human threats include such activities as theft, malicious damage, and tampering. Unauthorized maintenance is considered a form of tampering and is an important consideration for TEMPEST systems. Security measures to protect against intentional human threats fall into two categories:

1. physical security; and
2. access control.

You may consider tie down straps or lockable base plates as measures of physical security (17:--). Per AFR 205-1, you should add the computer system as an item of the nightly security inspection checklist (9:46; 23:A-1). AFR 300-6 requires you to account for the small computer system in the Automatic Data Processing (ADP) inventory. Be sure to work with your equipment custodian on this issue. AFR 300-6 also requires your ECO to be notified if you plan to move the small computer to another location. The only time the ECO does not need to be notified is when the move is part of an emergency plan (7:5-1).

AFR 205-1 requires you to implement access control measures for all small computer systems that process classified information (6:23). Access control options include such measures as seals, alarm systems, and secure office areas or secure buildings. You may consider having new locks put on your doors with the arrival of the small computer system. You should control the keys to the office (11:27; 17:--). Although these options address access control, you will find the principal form of access control is a series of administrative procedures as follows:

1. Monitor who has access to the general work area around the small computer system. Note strangers who come into the office since they may be casing the office.
2. Familiarize yourself with the maintenance clauses of the small computer contract before having any maintenance work performed on the system.
3. Don't let unauthorized personnel perform any maintenance on the small computer. This is critically important for TEMPEST systems since unauthorized maintenance can void the TEMPEST certification of the equipment. (See Chapter 5, "Maintaining TEMPEST Integrity", for more details.)
4. Be sure to keep a log of all maintenance performed on the system. This includes any maintenance work you may do yourself (26:--). (See Appendix B for a sample maintenance log.)

Unintentional human threats. Unintentional human threats include food, smoke, liquids such as water, coffee, or soda, and unintentional equipment damage. Physical shock and vibration also pose threats since repeated jars can loosen small contacts in the system and cause difficult-to-trace intermittent system failures (1:7). Security measures to counter these threats are based on common sense. Don't eat or drink near the small computer. Don't smoke around the system. Smoke, in particular, impacts reliability of floppy disk drives. Avoid bumping into the system. Keep printers and plotters and other vibrating devices separate from the small computer itself; this is particularly important for hard disk systems (1:10).

Lastly, educate yourself about small computers. Understanding a little about the system will go a long way in preventing inadvertent damage.

Environmental threats. We'll look at four kinds of environmental threats:

1. threats from the "normal" office environment;
2. electrical power surges and fluctuations;
3. bad weather conditions; and
4. the threat of fire.

Let's first take a look at problems in the "normal" office environment. Small computers are designed for the office environment, so they are not very susceptible to temperature and humidity variations. However, low humidity can cause static electricity which can produce difficult-to-trace intermittent system failures. Poor air quality (smoke and dust) can clog circuit board contacts and will eventually lead to intermittent failures. It can also clog cooling vents and lead to heat problems. Dust and dirt in disk drives can cause read/write errors or other disk failures. Heat buildup can cause intermittent failures. Overheating will also shorten the life of the components (24:7-8). To reduce static electricity problems, consider grounded floor matts and static electricity sprays; also consider a humidifier. Make sure all users are aware of the problem. If static electricity is a problem in the office, ground yourself before you touch the system. Consider air cleaners for the office if the air quality is poor (15:12). Clean system components regularly. Include disk drives, printers (a real dust producer), keyboards, and video screens. A vacuum cleaner can be used for cleaning many components, but be sure the computer is turned off before attempting to clean it (1:9). Commercial pressurized inert gases are available from computer dealers for cleaning keyboards. When cleaning video displays, be sure you use a lint-free rag (1:9). Don't spray the liquid cleaner directly on the display. Spray the liquid onto the rag. System fans are normally adequate to prevent heat build up; however, give the system adequate ventilation so the fan can work properly (15:12).

Electrical power surges and fluctuations pose another threat to the system. They may be standard features of your electrical support. They may also be the result of overloading the circuits. There are several measures to protect against these problems. First ensure the small computer is adequately grounded (1:8). Avoid using extension cords. Never use a three-prong to two-prong converter on any of the computer equipment. Recommend you use high quality power strips for the system. Do not put any appliance other than computer components on the strip. Use surge protectors between the system and the supply source. Keep "electricity hungry" appliances such as vacuum cleaners, electric heaters, and coffee pots off the same circuit as the small computer system. Remember this when the cleaners come in to vacuum the office. Recommend you turn off the system if the cleaners use the same circuit. If the electricity is generally "poor" in quality consider having engineers evaluate the electrical load and rewire if necessary.

Bad weather conditions, particularly thunderstorms, can threaten the system. Floods and tornadoes may also pose problems in your geographical area. If the office is susceptible to power interruptions during bad weather conditions, don't operate the computer during those times. If computer use is required during periods in which electricity is out, consider an Uninterrupted Power Supply (UPS) to provide the necessary power (15:11).

Fire also poses a threat to the system; however, it is not only the fire itself that threatens the computer, but also the measures we normally take to reduce fire damage. First, if you do not have a fire sensor system in the office, recommend smoke sensors. If the office has a sprinkler system, we recommend the small computer be located as far away as possible from the sprinkler since direct water contact when the sprinkler goes off will damage the system. Fire extinguishers can also pose problems. Do not use water to douse a computer fire. Water is most damaging and poses an electrical shock hazard for the user. CO2 extinguishers offer a better alternative; however, CO2 is toxic to humans in a closed area and can cause a video display to blow up if it is turned on. A halon extinguisher is the best solution for computer fires. We recommend acquiring these extinguishers when possible (15:13). You may consider checking with the base fire department to see if halon extinguishers are available through them. Lastly, if a fire should develop in the office, turn the system's power off.

Protecting the Software

For purposes of this handbook, we shall consider software as any standard, off-the-shelf software package that comes with the small computer system (such as Z-DOS, BASIC, or WordStar) and any applications program developed for the computer. We'll look at protection of this software from two perspectives: protecting the media on which the software is stored and protecting the actual software code itself. We'll not discuss procedures for safeguarding the software due to its sensitivity since these procedures are the same as those for data and will be discussed below in "Protecting the Data".

Protecting the media. Since floppy diskettes will be the primary media storing the software, we will limit our discussion specifically to protecting floppy diskettes. We realize you will also use cartridges and hard disks to store software; however, the general measures we are presenting also apply to those media.

Floppy diskettes face the same human and environmental threats as hardware. Without repeating these threats, let's discuss security measures to reduce the risks. These measures are based upon common sense. Do not take the diskette out of its jacket. Don't bend it. Don't touch the exposed surface of the diskette. Use only a felt tip pen when writing on either the jacket or a label on the jacket (24:5-9). Carefully follow the instructions for making copies of the original diskette and for installing the application (1:12). Store the diskettes vertically in a safe place to avoid loss or damage. Be sure to store the working copies of the software programs in a safe place when you are not using them (24:5-9).

Protecting the code. Since sensitivity protection of software is the same as that of data (see "Safeguarding the Data" below), we´ll limit our discussion to three points:

1. don´t modify software packages;
2. maintain control of the software through an accounting procedure; and
3. make backup copies of all software.

In looking at the issue of software modification, consider two kinds of software: standard, off-the-shelf software and software developed for the system. In the first case, do not modify any standard, off-the-shelf programs. The vendor will not be responsive to problems you might have if you modify his package. As with off-the-shelf software, do not modify applications programs developed for the system. The problems you may experience as a result of modifying the program (such as unexpected performance from the software or inaccurate documentation now that the program is changed) can far outweigh any advantages in modifying it. In some cases, such as those programs dealing with safety of flight, modification is forbidden.

Though not required by regulation, small computer software should be managed through an accounting procedure. We highly recommend the equipment custodian take up this responsibility. You should inventory all software belonging to the system. An inventory should consist of: name, version number, and serial number. You should also associate the software package with the serial number of the system. The inventory should be updated whenever new software is added to the system and when you receive updated versions of software packages. We cannot overemphasize the importance of this accounting procedure. In the long term, a software inventory will save you many hours of frustration. (See Appendix E for a sample software inventory.)

Lastly, be sure to back up all software. (See Chapter 5, "Backup Procedures", for details.) Although not required by regulation, consider having the equipment custodian monitor these backup procedures (26:--).

Safeguarding the Data

We are going to take a different approach in discussing security measures for safeguarding data. We´ll consider protection of both the media and the data itself. However, our discussion will focus on data protection from two perspectives: maintaining the integrity of the data (i.e. its accuracy, correctness and completeness), and safeguarding the data due to its sensitivity. A point to remember - security measures for protecting the data media is the same as that discussed above in "Protecting the Software". We´ll not repeat these measures again, but do remember they also apply to data protection.

Maintaining data integrity. Data integrity is threatened in three ways: the data is accidentally lost; the data exists but cannot be found on the medium; and data is incorrect due to data entry mistakes. In addition, accidental data loss includes exposure of the medium to a magnetic field; accidental erasure of data by incorrectly applying writing or copying procedures; inadvertently overwriting data not permanently stored elsewhere; and losing or damaging the data medium. There are a number of security measures to reduce the various integrity risks:

1. Keep diskettes, cartridges, and hard disks away from magnets and degaussers. Keep them at least a foot away from any electrical appliance. Do not put diskettes or cartridges next to video displays. Do not put them on top of disk drives (14:8).
2. When appropriate, use write protect labels on the diskettes to prevent overwriting the data.
3. When appropriate, write protect data files if the utility is available through the operating system or an applications package (1:23).
4. Establish procedures for tracking the information stored on the data media. Some operating systems provide tree-structured directories to help in managing the information on the medium. (Before implementing a convention such as this, be sure you understand the limitations of the applications software in handling the file management convention.) Consider a short log of file name and file contents for each diskette, cartridge, and hard disk. (A sample log is provided as Appendix C.)
5. Establish file name conventions so that contents of the file are apparent from the file name (24:5-14). If you share hard disks or cartridges, you might consider a standard file naming convention where all files belonging to one owner have the same filename extension (e.g., owner's initials).
6. Establish backup procedures and maintain backup copies of the data (see Chapter 5). Consider making the equipment custodian responsible for managing the routine backup and storage of the data. Keep in mind storage media does not last forever. Heavily used floppy diskettes can "wear out" after thirty or forty days of hard use (26:—).
7. Become familiar with the system. Understand how the software packages work. Education can help eliminate problems with data loss and data entry mistakes.

Safeguarding sensitive data. The data must be protected commensurate to its sensitivity (6:20). Several Air Force regulations dictate the requirements for protecting data. AFR 205-1 presents Air Force requirements for safeguarding classified information. AFR 12-35 addresses data protected under the Privacy Act of 1974. AFR 205-16 and AFR 300-13 expand on these general directives as they apply to computer systems. In the following discussion, we will assume you are familiar with the requirements of AFR 205-1 and AFR 12-35. We shall frequently refer to AFR 205-1 since this regulation applies to all small computer printouts (any hardcopy from the printer, plotter, etc.).

The major threat to sensitive data is intentional or unintentional access to the data. For standalone small computer systems we have two measures to counter this threat:

1. use of TEMPEST equipment; and
2. procedures for controlling access to the data.

Using TEMPEST equipment. Let's first look at using TEMPEST equipment. Data processed on any computer can be compromised because the system may electromagnetically emanate signals such that the data being processed can be intercepted. Use of TEMPEST equipment can reduce this risk (17:--). The need to use a TEMPEST small computer should have been determined during the planning phase of the system. The local TEMPEST officer should have helped determine the TEMPEST requirements based upon your needs for processing sensitive data. If the small computer system is TEMPEST equipment (such as the Air Force standard TEMPEST Zenith Z-150 system) you have taken a major step in protecting your sensitive data; however, having a TEMPEST system does not entirely eliminate the risk of emanations. There are environmental constraints on using TEMPEST equipment (8:5-2). For example, you may need to locate a TEMPEST system such that it is not near telephone lines or water pipes. You must check with the local TEMPEST officer before you start using TEMPEST small computers in the office to ensure all environmental constraints have been addressed in locating the equipment. There are other considerations that must also be addressed in maintaining the the TEMPEST integrity of a TEMPEST system. Chapter 5 presents a more detailed discussion of procedures to be followed to ensure TEMPEST integrity.

Controlling access to the data. Whether or not the system is TEMPEST certified, you must follow procedures for controlling access to sensitive data. There are several ways to protect sensitive information on computer systems: use of passwords and encryption techniques, media labelling, and physical data segregation (3:69). As we mentioned earlier in this chapter, one of the major vulnerabilities of a small computer is its lack of internal hardware and software mechanisms to prevent access. Unfortunately, Air Force approved password and encryption schemes are not generally available on small computer systems to counter this vulnerability. To control access to sensitive data we must rely on:

1. media labelling; and
2. segregation procedures.

We'll not discuss procedures for labelling the media here since procedures for marking computer data media are discussed in Chapter 5, "Sensitivity Markings". We will, however, address various security measures for segregating the data to reduce the risk of unauthorized access.

To segregate the data we must address two areas:

1. system security measures; and
2. media security measures.

Let's look at system measures first. The small computer system must be located to limit viewing of the video display and printed output when it is in use. You must implement physical security and access control as discussed above in "Protecting the Hardware". You must also operate the system under the dedicated security mode which requires all users of the system to have both the clearance and the need-to-know for all the data that resides on the system. (See Chapter 5, "Mode of Operation", for details on how to operate in this mode.) When the system is not located in a controlled area (i.e., an area approved for open storage of classified information), you must declassify the system when changing sensitivity level of the system to a lower level (e.g., going from processing top secret information to processing only confidential information) or when leaving the system unattended. There are also declassification requirements before moving the system and before allowing maintenance to be performed on it. (See Chapter 5, "Declassification Procedures", for details.)

Security measures for treating data media (floppy diskettes, hard disks, cartridges, etc.) are also required. The requirements of AFR 205-1 apply here. Media is generally treated like sensitive documents. You must apply the requirements of AFR 205-1 and AFR 205-16 in: marking the media; storing the media; transferring the media to other offices, agencies, etc.; viewing the data stored on the media; and declassifying the media. Requirements for marking the media are described in AFR 205-16 and are discussed later in this handbook in Chapter 5, "Sensitivity Markings". Media, to include floppy diskettes, hard disks, cartridges, and printer/plotter ribbons, must be physically stored following the same security requirements used to store documents of the same sensitivity level. Any receipting, log maintenance, etc., required for sensitive document control also applies to the data media. Viewing of the data on a video display is no different than viewing a document. If administrative procedures are required for viewing the document, those same procedures apply to viewing the data stored on magnetic media as well. Procedures for declassifying the media also apply. (See Chapter 5, "Declassification Procedures", for details.)

In addition to the above requirements, there are procedures to be followed in handling the data media when the system is in use. First, you must maintain separate sets of media for unclassified and classified data processing. This means you must have two sets of media to "boot" the system as well as two sets of media with the applications programs. This also means you must have, at a minimum, two sets of media for storing data and two sets of printer ribbons as well. You may share these media with other users; however, all users of the media must have authorized access (i.e., security clearance and need-to-know) to all the information residing on the media. Lastly, you must protect all the output from the system at the system sensitivity level until the output data has been reviewed and marked with its actual sensitivity. For example, if the system is processing at a secret level, all the output from the printer (as well as the data storage media) must be treated as secret until you have reviewed the data and determined it to be unclassified.

Other Related Issues

There are several related security issues we need to address in operating a small computer system. These include: software duplication, both documentation and supplies considerations, computer abuse, use of personally owned computers, processing personal data on small computer systems, appointment of both a security officer and an equipment custodian, and, lastly, the approval to operate the small computer system. Let's look at each of these issues, one-by-one.

Duplication of software. Generally, off-the-shelf software is not bought by the Air Force, but rather is licensed to the Air Force for its use. To date, there are no Air Force-wide licensing agreements for any off-the-shelf applications software (such as WordStar or dBASE II) for general use on Air Force small computer systems. Normally, the software is licensed by small computer system. For example, all standard software acquired from the two Air Force standard contracts with Zenith Data Systems is licensed by the small computer system for which it was bought. This means you can only use the software on the system for which it was purchased. It would be illegal for you to copy WordStar acquired for your Zenith Z-150 system for use on another Z-150 located in another office because that office did not buy WordStar for their system. The specific licensing restrictions may differ depending on what software was bought and how it was acquired. If you have any doubts, be sure to contact the SI personnel. Another point to consider is the creation of backup copies of the licensed software packages. Unless specifically prohibited by the vendor, making backup copies of software is legal and encouraged. Consider how many copies you need to provide adequate backup capabilities. (See Chapter 5, "Backup Procedures".) In any case, remember unauthorized copying and distribution of copyrighted or licensed software is prohibited (20:--).

Documentation. Software documentation needs protection as does the software itself. This includes not only programmers' documentation but user's manuals as well (1:17). Be sure to consider safekeeping of the documentation. Also, remember to consider documentation requirements in contingency planning (see Chapter 2).

Supplies. Although small computer supplies are not generally considered part of the system itself, their protection is important since they are particularly vulnerable to theft (24:5-13). Be sure to provide adequate security measures for small computer supplies.

Computer abuse. AFR 30-30 addresses computer abuse and states that Air Force resources shall only be used for officially approved activities (13:4). AFR 205-16 specifically prohibits misuse of small computer systems. Misuse applies not only to the hardware, software, and supplies, but includes computer time as well (6:8). If you have any doubts as to which activities are considered authorized computer use, contact the SI personnel for clarification.

Use of personally owned computers. AFR 205-16 prohibits the use of personally owned small computers if one or more of the following conditions apply: the system processes sensitive, unclassified information; the system processes classified information; or, the system is a critical resource (criticality of ADP-I or ADP-II) (6:8-9). Though the use of a personally owned small computer is not prohibited for processing non-sensitive, unclassified information, it is highly discouraged since it can easily lead to problems of dependency and maintenance responsibilities (26:—).

Personal data on small computer systems. As we defined in Chapter 2, personal data includes Privacy Act data as well as other private data such as medical or legal information. Processing this sensitive data on small computers needs special attention. Though the risk of disclosure or alteration is low, small computer users tend to overlook the constraints imposed on processing personal data on computers (12:3-5). These limitations include:

1. restrictions on when the data can be kept;
2. requirements on keeping the data current; and
3. reporting requirements for systems that process personal data (5:2).

Though our intent is not to make you an expert in personal data processing requirements, you must be aware that restrictions exist in processing personal data on small computer systems. Keep that in mind when you use a small computer. If you have a question about the matter, contact the administrative personnel.

Appointment of a TASO. One of the most important considerations when a small computer system arrives is the appointment of a TASO for the office systems. Be sure a person is appointed immediately. As mentioned in Chapter 2, this person is responsible for maintaining the security of the office's small computer system(s).

Appointment of an equipment custodian. Another important consideration when the small computer arrives is the appointment of an equipment custodian. This person is required by AFR 300-6 to assist the ECO in maintaining an inventory of the hardware (see "Protecting the Hardware" above). He or she should also maintain an inventory of all its software (see "Protecting the Software" above) and be responsible for backup procedures for both the system's software and data (see Chapter 5, "Backup Procedures").

Approval to operate the small computer. In Chapter 2, we identified the DAA as an individual key player you should know. Before you can use a small computer either to process sensitive or classified information or to process critical applications, you must have the written approval of the DAA. Be sure you have this approval before you use the system. If you are not sure who the DAA is, check with the SI personnel.

Summary

In this chapter we have taken a look at small computer security in terms of its hardware, software, and the data it processes. We have discussed security in terms of vulnerabilities and threats and security measures to counter the associated risks. We've also discussed several other security issues related to the use of small computer systems. In the next chapter we will discuss a number of recurring security procedures to be followed when operating a small computer system.

CHAPTER 5

"I´m ready to turn it on. So . . ."

Introduction

In this chapter we will discuss recurring security procedures you´ll be using with a small computer system. The procedures reflect current Air Force policy for small computers. Though the information provided in this chapter may be redundant with other chapters of this handbook, the intent is to consolidate these recurring procedures into one section. The chapter will specifically address the following areas: system sensitivity level, mode of operation, maintaining the TEMPEST profile of a TEMPEST system, sensitivity markings, backup procedures, declassification procedures, destruction procedures, and general operating procedures. In each case, we shall first present a general discussion followed by specific procedures.

System Sensitivity Level

In Chapter 2, we defined system sensitivity level as the highest level at which sensitive software or data is being processed, stored, used, or produced on the small computer system. Let´s now expand that definition. In talking about system sensitivity level, we must first define the system. The system is considered the small computer itself and all the peripheral devices connected to it. It includes the keyboard (if a separate item), the video display, the printer, the plotter, and any other device physically connected to it. The system sensitivity level is the highest sensitivity level of any software or data that has been processed, stored, used, or produced on the system since it was last declassified. Thus if you input top secret data from the keyboard on an otherwise unclassified system, the system sensitivity level is now top secret. If you are working on secret information but the cartridge you are using has top secret data stored on it, the system sensitivity is top secret. Pay particular attention to printer/plotter ribbons. You may think the system is unclassified, but if you have a secret ribbon in the printer, the system sensitivity is secret.

Mode of Operation

As we defined in Chapter 2, a mode of operation is the manner of operating the small computer system to process, store, use, or produce sensitive or classified material. There are actually four modes of operation for computers: the dedicated security mode, the system high security mode, the controlled security mode, and the multilevel security mode (6:9). A detailed explanation of these modes is provided in AFR 205-16. You can look there for specific characteristics of these operating modes. Our only concern here is the dedicated security mode. As we stated earlier in Chapter 4, the dedicated security mode is the only approved mode of operation for operating single-user, standalone small computers. In the dedicated security mode, the small computer and its peripherals are used for processing sensitive or classified information and controlled by an exclusive set of users. All the users of the system must have both the security clearance and the need-to-know for all sensitive and classified data residing on the system. The other modes of operation are not applicable to the small computer because these modes require internal control features to limit user access to information, features generally not available in either small computer hardware or standard, off-the-shelf software. The dedicated security mode satisfies our needs since in this mode we can administratively control access to the sensitive information (6:17; 25:--).

Maintaining TEMPEST Integrity

If the small computer is a TEMPEST system, you need to be aware of several security considerations in maintaining the TEMPEST profile of the system. Four specific points to keep in mind are:

1. operating procedures;
2. connection of the system to other equipment;
3. environmental changes; and
4. computer maintenance.

First, you must follow all operating procedures in using the system. If the system has special doors or lids because of its TEMPEST certification, you must be sure they are being used correctly when operating the system. For example, printer lids must be down when processing sensitive data on a TEMPEST machine. A second consideration is the system configuration. When you plan to process classified information, do not connect a TEMPEST small computer to any peripherals that are not also TEMPEST certified. If you are in doubt, check with the TEMPEST officer. If you connect a TEMPEST system to non-TEMPEST equipment you cannot process classified information because you have compromised the TEMPEST integrity of the system. You must also be aware of environmental changes that can invalidate the TEMPEST integrity of a system. When your system was installed you worked with the local TEMPEST officer to ensure the environment did not compromise the TEMPEST system. If the office environment has changed since you installed the system, check with him again. For example, if you have had new phone lines put in since the system was installed, check with the local TEMPEST officer to ensure there is no impact on the system's TEMPEST integrity. If you plan to move a TEMPEST system, again you must check with the local TEMPEST officer before making the move. Th last consideration is maintenance of a TEMPEST system. Only authorized personnel are allowed to maintain a TEMPEST system. Attempts by anyone other than those authorized to maintain TEMPEST equipment is considered tampering and can compromise TLMPEST integrity. Unauthorized personnel may include yourself. Though you may be familiar enough with the equipment to perform minor maintenance, you may not be authorized to do so. Unlike non-TEMPEST systems, you cannot swap boards, change cables, or do other simple procedures in trying to fix a problem. If you are not sure about the maintenance arrangements for the system, find out from the SI personnel. For example, Honeywell has been awarded the maintenance contract for the Air Force standard TEMPEST Zenith Z-150. Only Honeywell personnel can perform maintenance on the Zenith Z-150. When maintenance personnel come in to fix the system, be sure to verify their clearance and their authorization to work on the system. (Check with the security officer for your area for clearance and access requirements.) Lastly, maintain a log of all maintenance performed on a TEMPEST system. The log should include a simple explanation of the maintenance problem, the date of repair, the name of the serviceman making the repair, and the action taken to correct the problem (23:A-4 - A-5; 26:--; 18:1-2). (See Appendix B for a sample maintenance log.)

Sensitivity Markings

A small computer must be marked to designate the highest level of sensitive data processed, stored, used or produced on the system. Specifically, you will need to mark all software and data media used on the system. That includes magnetic media, printer/plotter ribbons, and hardcopy outputs. Don't forget sensitivity markings are required for all sensitive software and data. This means not only classified software and data, but personal software and data as well.

Let's first discuss sensitivity markings for magnetic media. The same marking requirements apply when the media is storing either software or data. The media must be marked at the highest sensitivity level of any software or data recorded on it since it was last declassified. Specific marking requirements reflect those of AFR 205-1. The sensitivity must be marked as well as the classification source, the downgrading instructions, and all other markings required by AFR 205-1 (9:Ch 4,Ch 11). In addition, the media should be marked to identify ownership and general contents. (See Appendix D for examples.) If a small computer system is authorized to process both unclassified and classified data, all its media must be marked for sensitivity even if the media unclassified. One last point to remember, keep all markings unclassified (6:24-25 and 23:Exhibit-1).

You must also mark all hardcopy outputs the small computer produces. You must mark the output as you would any document, following the procedures as specified in AFR 205-1 (9:Ch 4,Ch 11). Confidential and secret printcuts used in preparing finished documents are classified as working papers and are treated as such. Top secret printouts, regardless of their use, are classified as finished products and treated according to the requirements of AFR 205-1 (6:23-24). One last point to remember - until computer hardcopy products have been reviewed and marked for their actual sensitivity, they must be treated and safeguarded according to the system sensitivity level.

Backup Procedures

As stated in Chapter 3, a contingency plan establishes procedures for dealing with unexpected small computer losses. We deal specifically with losses of software and data in backup procedures. The importance of implementing backup procedures cannot be overemphasized because these procedures provide you the capability to reconstruct applications programs and data when either is lost or unusable. The procedures are mandatory for systems with a criticality of ADP-I or ADP-II (see Chapter 3, "The Risk Analysis"). However, backup procedures should be established and routinely used regardless of the system's criticality. Let's now look at software and data backup procedures.

Software backup. Several-rules-of-thumb apply in backing up software. These rules address:

1. copies of applications programs;
2. backup copies of programs needing installation;
3. storage of backup media;
4. software documentation; and
5. software code.

First, you should maintain at least one backup copy of every applications program you have for the system. This means copies of the operating system, off-the-shelf software packages such as WordStar or dBASE II, and any other applications software. All software master diskettes should be treated as backup copies. (Never use the master as a working copy of the program. You always want the ability to recover from the master program when all else fails. You may also need the original diskette for update purposes when dealing with the vendor.) At least one copy of all software developed for the system, regardless of the level of effort in its development, should be maintained as a backup. Thus a simple BASIC program to track suspenses should be backed up as well as a mission planning package developed under a multimillion dollar contract. Also remember to maintain a backup copy of new versions of software and software modifications. Second, for software packages requiring installation, make a backup copy of the installed version of the program. For example, WordStar can be customized through its installation package. You can save yourself considerable recovery time by recovering with an installed version of WordStar rather than using the master WordStar diskette which will require reinstallation for recovery. Third, be sure to store all the backup media in a safe place. You do not want the software to be lost or stolen. In picking a location for storing the media, you will need to weigh your need for accessibility to the backup software against the need to protect the software from human and environmental threats (theft, fire, etc.). Next, don't forget to consider your need for backing up software documentation. Make copies of the documentation when you can and store them in a safe place. However, we are not suggesting you break copyright laws and illegally copy vendor-supplied documentation. Lastly, keep a hardcopy of the code to all applications programs for which a hardcopy is available. Store these printouts in a safe place.

Data backup. A critical step in backing up data is selecting a set of procedures that satisfies your requirements. In selecting procedures to suit your needs, you'll need to consider:

1. the value of the data;
2. the backup alternatives available;
3. the amount of data to be backed up; and
4. the media storing the data.

First, you must consider the importance of the data. Not every piece of data you have is valuable enough to back up. For example, you probably do not need to back up a one line letter responding to a suspense; however, the budget data base for a $15M project is important enough to back up. You'll also find that the value of the data will determine how often it should be backed up.

Next, consider the various backup alternatives on the market - floppy diskettes, cartridges, hard disks, streaming tapes, and others. Hardcopy is also an alternative, but usually a last resort. You may be limited to alternatives available to you due to cost constraints. Some backup technologies are more expensive than others.

You must also consider the media on which the data currently resides in selecting a backup alternative. If you store data only on floppy diskettes, your decision is simple. However, if you use hard disks and cartridges to store the data, you'll need to select an alternative that allows you to copy the data from that source to a destination media. The destination of the data may not be the same media as the source media. Be sure not to get trapped into getting a backup system that provides a great hardware alternative, but does not have the necessary software utility to perform the backup function. For example, don't get a streaming tape backup system if there is no software available to copy the data from the cartridge onto the streaming tape.

Lastly, in selecting an alternative, you'll need to consider the volume of data to be backed up. Generally, if you are dealing with a large amount of data, cartridges and streaming tapes are good alternatives because they are fast. Use of floppy diskettes is always an alternative, but not necessarily an attractive one because backup is fairly slow when dealing with large volumes of data. (If floppy diskette backup is the only viable alternative, do not despair. Today's operating systems allow you to copy from one floppy diskette to another. Many also provide a standard utility for backing up a cartridge or hard disk to floppy diskette. Some utilities allow you to discriminate by time of the last update, an important capability since it allows you to selectively back up only data that has changed since the last backup. In evaluating floppy disk backup utilities, beware of routines that copy data on floppy diskettes in an unreadable format. In that case, you can only restore that data on the original media and not read the data on the floppy diskette.)

Once you've selected a backup procedure, you'll need to decide where to store the backup data. You must weigh the same two factors for storing either software or data - accessibility versus protection from human and environmental risks. Don't forget sensitivity of the data poses an additional constraint on storage requirements. The data must be protected commensurate to its sensitivity.

The actual procedures will depend on the backup alternative you select and implement, but, in short, selecting and using backup procedures can be summarized in four steps:

1. determine what data needs backing up and how often backup is required;
2. select an available backup method suitable to your needs;
3. backup the data as required, copying only data that has changed since the last backup if that selective capability is available; and
4. store the backup media in a safe place, considering sensitivity requirements when applicable.

Let's make one last point about backing up data. Though not a specific consideration in selecting and implementing a backup alternative, you should remember a very important rule-of-thumb: the time it takes to back up the data is not the determining factor of when or how often you should perform the backup procedure. The value of the data should be the only factor influencing that decision. Too many times people fail to back up their data because the procedure is a tedious one. Rest assured, sooner or later you will regret saving those few minutes by not backing up the data.

Before closing the discussion of backup procedures for software and data, recommend you consider having the equipment custodian be responsible for backing up and storing all the software and data. Though not required by regulation, putting the equipment custodian in charge of software and data management will make the general management of the small computer system simpler (26:—).

Declassification Procedures

Two procedures exist to eliminate classified information from computer systems - clearing and declassifying. Clearing consists of simply overwriting or erasing the classified information residing on the computer system (6:20). It is of limited value since a cleared system may still have residual effects of the classified information and must still be treated as a classified system and safeguarded accordingly. For example, as a clearing procedure, a user may "erase" a file stored on floppy diskette by using a "delete" function. He or she has performed an "erase" function, but in reality the only data erased is the pointer information in the directory of the floppy diskette. The file still exists on the diskette and the data can oftentimes be recovered. However, a system that has been declassified has no residual effects of classified information and can be treated as unclassified once the procedure is completed. All small computer systems must be declassified to prevent the unauthorized disclosure of residual classified information. Clearing is not an acceptable alternative for declassifying a small computer (26:—).

Declassification procedures apply to both the small computer system and to the media used to store sensitive software and data. For purposes of declassification, a system consists of all system components except software or data media (floppy diskettes, hard disks, cartridges, printer/plotter ribbons, and hardcopy). Thus, a system consists of all central processing unit (CPU), registers and memory, the video display, and other peripheral devices (printer, plotter, etc.). It also includes floppy diskette drives, but not the floppy diskettes themselves. There are separate declassification procedures for the various software and data media.

When you must declassify. There are particular instances when the system and the media must be declassified. As mentioned in Chapter 4, if the system in not located in a controlled area and the system has processed sensitive information, the system must be declassified if one of the following conditions exist:

1. you are changing sensitivity level of operation to a lower sensitivity level (for example, going from processing top secret to secret or from secret to unclassified); or
2. you are leaving the system unattended.

Regardless of where the system is located, you must declassify it when:

1. maintenance personnel are planning to work on the system; or
2. when you are moving the system to another location outside the office.

Media must be declassified when the sensitive software or data can no longer be safeguarded (6:20; 26:—).

System declassification procedures. System declassification procedures mainly consist of turning off the system and logging the declassification. This procedure applies only to small computer systems in which all system components have volatile memory. If you are not sure about the system, check with the SI personnel. If the system has any non-volatile components, the following declassification procedures no NOT apply. You will need to establish acceptable declassification procedures with the ISSO. Please note all equipment from the Air Force standard Zenith Z-100 and Z-150 contracts have volatile memory and the following declassification procedures apply (17:—).

Specific system declassification procedures are as follows:

1. Remove and safeguard all sensitive media. This includes magnetic media, printer/plotter ribbons, and computer printouts.
2. Turn the video display control to its maximum brightness. Turn off all system components except the video display. Wait five seconds. Turn off the video display.
3. Log the declassification date, time, and individual accomplishing the declassification. Get a witness's signature of the declassification procedure. (Per AFR 205-16, this log must be maintained for a period

of two years.) See Appenaix A for a sample declassification log.

NOTE: If you plan to use the system again, be sure ten seconds have elapsed before turning the components back on (6:20-22; 26:--).

Media declassification procedures. Media declassification procedures depend upon the medium being declassified. There are different declassification procedures for:

1. magnetic media;
2. printer/plotter ribbons; and
3. hardcopy.

Magnetic media. We'll discuss two declassification procedures for floppy diskettes and then discuss how these procedures apply to other magnetic media such as hard disks, cartridges, and magnetic tapes.

The two methods for declassifying floppy diskettes are:

1. degaussing procedure; and
2. overwriting procedure.

A floppy diskette can be declassified using an approved tape degausser. (See the ISSO for a current list of NSA approved tape degaussers.) The SI personnel can tell you the actual procedures for using a degausser. After degaussing the diskette, change the sensitivity marking on the diskette. Log the declassification date, time, and individual accomplishing the declassification. Get a witness's signature of the declassification procedure. (Per AFR 205-16, this log must be maintained for a period of two years.) See Appendix A for a sample declassification log.

If tape degaussers are not available, an overwriting procedure can be used. The procedure consists of reformatting and writing over the diskette three times. The actual procedure consists of the following steps:

1. reformat the sensitive diskette;
2. copy the entire contents of an unclassified, non-sensitive diskette onto the diskette you are declassifying;

NOTE: If a "DISKCOPY" or similar type command that automatically reformats the target diskette is used, you do not have to reformat the sensitive diskette before copying.

3. repeat these first two steps two more times;
4. compare the contents of the two diskettes to ensure they are identical;
5. change the sensitivity markings on the diskette; and
6. log the declassification date, time, and individual accomplishing the declassification. Get a witness's signature of the declassification procedure. (Maintain the log for a period of two years.)

If neither tape degaussers nor reformat/copy procedures are available, the floppy diskettes cannot be declassified. In that case, you must safeguard the diskettes to the degree commensurate with the highest sensitivity level of data ever stored on them until the diskettes are destroyed (6:21; 26:--).

Other magnetic media such as hard disks, cartridges, and magnetic tapes can generally be declassified using either a degaussing or overwriting procedure. However, several points should be considered. First, use of a tape degausser on a hard disk can erase timing and formatting data and render the device inoperable. Do not consider this approach a declassification alternative. Second, you may be limited by software in your ability to reformat and copy an entire hard disk, cartridge, or magnetic tape to another like medium. If the capability to reformat, copy, and verify do not exist in standard software, there is no valid overwriting procedure available for you to use. Third, be sure when you declassify the media you log the date, time and individual accomplishing the declassification. Get the signature of a witness and maintain this declassification log for two years. And lastly, remember, once the media has stored sensitive data, you must safeguard it to the degree commensurate with the highest sensitivity level of data ever stored on it until it is destroyed (6:21; 26:—).

Printer/plotter ribbons. Declassification procedures for printer/plotter ribbons are quite simple. A film ribbon cannot be declassified. A printer/plotter ribbon which can be overwritten can be declassified when it is consecutively overwritten with unclassified, non-sensitive information five times. Mark the new sensitivity of the ribbon and log the declassification date, time and individual accomplishing the declassification. Get a witness's signature. (Maintain this log for a period of two years.) If a sensitive ribbon is not declassified, it must be safeguarded to the degree commensurate with the highest sensitivity level of data ever printed with it until it is destroyed (6:20-22).

Computer hardcopy. All computer hardcopy products are declassified according to the declassification procedures specified in AFR 205-1 (9:Ch 3,Ch 11).

Destruction Procedures

All software and data media (floppy diskettes, hard disks, cartridges, magnetic tapes, printer/plotter ribbons, etc.) are subject to the same destruction procedures. If the media stored unclassified material, it will be burned since it will generally contain sensitive information. All classified media will be destroyed according to the standard destruction procedures for classified data. If you have doubts on how to destroy media, particularly hard disks and cartridges, check with the ISSO (6:22; 26:--).

General Operating Procedures

In this section we shall briefly go through what must be considered in operating a small computer system. We´ll first discuss operating constraints, then walk through what must be remembered to begin processing, during processing, and to end processing. First, we´ll take a look at operating constraints.

Constraints on operating the system stem from your need to protect sensitive and classified data and, as a consequence, from system declassification requirements. You cannot arbitrarily process data of differing sensitivity levels. As discussed in "Declassifying Procedures" above, there are specific times when you must declassify the system. Keep these declassification requirements in mind when you begin processing sensitive data. Once you´ve processed sensitive or classified information you must declassify the system before unclassified processing can begin. You can go from processing secret data to processing top secret data without declassifying the system; you cannot do the reverse without declassifying. Lastly, you can go from unclassified processing to classified processing without any declassification procedure; however, the system is to be rebooted with the classified set of software. With these operational constraints in mind, let´s now take a look at the general procedures to begin processing.

There are three steps to begin processing.

1. determine the sensitivity level of the system;
2. insert the appropriate ribbon(s) into the printer and plotter; and
3. boot the system using the appropriate set of software.

At this point you are ready to begin processing. Now let´s examine the processing phase of operation.

There are four considerations to be kept in mind when you are processing sensitive or classified information on the system:

1. use the data media you need for processing at the sensitivity level you have designated;
2. be sure you are controlling access to the system when you are processing sensitive or classified information;
3. if you are processing classified data on a TEMPEST machine, be sure you are maintaining TEMPEST integrity; and
4. when you are processing sensitive or classified information, be sure to monitor all computer printouts and safeguard these products at the system sensitivity level until the actual sensitivity level of the products are determined.

We are now ready to look at the last phase, ending computer processing.

Two points are key to end processing:

1. remove and store all data media; and
2. declassify the system if required.

If you do not need to declassify the system, all you do is turn the small computer off.

Summary

In this chapter we have taken a look at a number of recurring procedures you'll need to follow in maintaining security on a small computer system. Specifically, we have discussed system sensitivity level, mode of operation, maintaining TEMPEST integrity, sensitivity marking procedures, backup procedures, declassification procedures, destruction procedures, and general operating procedures.

At this point, you should know enough to safely maintain the security of a small computer system. However, we recommend you continue to read on. In the next chapter, we'll briefly discuss security considerations in relation to interfacing a small computer system. Although this handbook is designed for standalone small computers, this next chapter will highlight a couple important security issues. Appendices A through E should be helpful since they provide various examples and sample logs you'll be needing. Appendix F should be particularly useful since it is designed as a simple checklist in planning for and operating a small computer system.

CHAPTER 6

"I want to connect this computer to something. What must I worry about?"

Introduction

Although this handbook is designed only for standalone small computer systems, it will not hurt to spend a few minutes talking about communications and the impact it has on computer security. We do not intend to make you a communications expert, but we do hope to make you aware of serious security implications when communicating with a small computer system. We'll present a brief discussion of communications and security and then offer four possible scenarios for interfacing a small computer system. Let's begin with a few words on communications security.

Communications - The Weak Link in Small Computer Security

The capability for small computers to communicate through various communications links poses serious threats to data security and is considered a major vulnerability of small computer systems (4:98). In fact, the networking capabilities of small computers has been described as "open[ing] up a whole new Pandora's box" (4:98). Regardless of the communications approach used to allow the small computer to communicate - telephone lines, networks, direct links to other computer systems - the ability to communicate threatens the security of the data the small computer maintains. AFR 205-16 presents a general discussion of communications interfaces. It presents the communications security issue as one of safeguarding sensitive data. There are security implications in safeguarding sensitive and classified data once you have connected a small computer to an external device. This concern prevails at both ends of the communications link, the sensitive data the system processes and maintains and the sensitive data the system you are connecting to processes and maintains. The weakest link, of course, is the transfer of the data. Per AFR 205-16, the transfer of classified data requires physically protected or encrypted communications links, two security approaches readily available to the small computer user (6:8). With this communications weakness in mind, we will look at four interface scenarios in the next few paragraphs and present general constraints and guidelines. The four possible situations when interfacing a small computer are as follows:

1. your system is unclassified and the other system is unclassified;
2. your system is unclassified and the other system is sensitive or classified;

3. your system is sensitive or classified and the other system is unclassified; and,
4. your system is sensitive or classified and the other system is sensitive or classified.

We'll look at both systems processing unclassified data first.

Situation 1 - your system is unclassified
the other system is unclassified

There are no security issues that need to be addressed with this scenario. From a data security point of view, interfacing the system is acceptable whether you access a telephone line, a local area network (LAN), the Defense Data Network (DDN), or another communications link. However, you should work with the SI folks before deciding on a communications approach for the small computer. Much work is being done in standardizing communications links, particularly LANs for small computer systems. Don't get started on a communications project on your own without first touching base with SI personnel.

Situation 2 - your system is unclassified
and the other system is sensitive or classified
Situation 3 - your system is sensitive or classified
the other system is unclassified

These two scenarios are security nightmares. DON'T DO IT!!! In either case, you would be compromising the security of the system processing sensitive or classified data. Don't even consider a connection of this type. Talk to the SI personnel about your requirements and work on a solution to satisfy your needs.

Situation 4 - your system is sensitive or classified
the other system is sensitive or classified

Disregarding the communications aspect, this scenario may be acceptable if the security aspects of dealing with the sensitivity levels of the systems can be satisfied using an appropriate mode of operation. When you include the communications link, the scenario can still be acceptable if the communications technique for transferring the data does not compromise the sensitivity of the data, e.g., use of encryption or physically protected communications links. However, as we mentioned earlier, encryption and physically protected communications links are neither popular nor low cost approaches to small computer communications security. In addition, there are other considerations to be taken into account. For one, when you interface to a classified system, you must meet all the security requirements of that system. For example, if you want to connect to the World Wide Military Command and Control System (WWMCCS), you would be considered a terminal on that system and the small computer must meet all the security requirements of a WWMCCS terminal. In addition, you would have to get approval from the WWMCCS DAA to link to the system. The issue of TEMPEST integrity may also arise. If the classified system requires TEMPEST equipment, the system you use must also be TEMPEST. If it is not, it will compromise the TEMPEST integrity of the system with which you plan to interface.

We do not mean to paint you a gloomy picture of this scenario. We realize this is probably the scenario you will be wanting to implement. It is by no means an impossible scenario. Many Air Force small computer systems today operate under this situation. With the fielding of the Air Force standard TEMPEST small computer, this scenario is becoming an everyday occurrence. Physically protected or encrypted links may not be needed to satisfy security requirements. It may be possible to interface your sensitive system to another sensitive system in a timely and low cost fashion. However, we want you to be aware there are serious security implications in attempting such a connection. When you get a requirement such as this, be sure to work with the ISSO and the SI personnel to resolve security problems and develop a workable solution.

Summary

It is not impossible to connect a small computer to other systems and still maintain system security; however, you cannot arbitrarily do it on your own. When in doubt, check with the ISSO. If you identify a new requirement to communicate with other systems, work with the SI folks in clearing up computer security issues and coming up with a workable solution that satisfies your requirements. As more and more small computers are fielded, security issues are going to continue to crop up. In time, we'll have answers for alot of them. Just remember, don't try to tackle them alone. Work with the right people - the SI personnel and the ISSO. Don't compromise security integrity!

CHAPTER 7

"Hope this handbook has been helpful."

Closing Remarks

Our goal was to make you aware of your responsibilities in maintaining security on small computer systems. We hope with the past six chapters we have done just that. We´ve discussed security considerations in both the planning and operational phases of a small computer´s life cycle. We´ve also provided you with a number of security procedures you will be using routinely in working with a small computer system.

We hope you are happy with the handbook. But we won´t know unless we here from individuals who have used the handbook on a day-to-day basis. We would like to hear your comments, both good and bad and would be glad to answer any questions you might have. Please address all questions and comments to the following address:

AFTPC/CK
Gunter AFS, AL   36114

If you have a question that needs immediate attention, you can reach us at the following number:

AUTOVON: 446-4068

BIBLIOGRAPHY

A. REFERENCES CITED

Books

1. Lyons, Norman B. Understanding Computer Crime. Sherman Oaks, California: Alfred Publishing Co., Inc., 1984.

Articles and Periodicals

2. "Computer Break-Ins Fan Security Fears." Science, Vol. 221, No. 4614: pp. 930-931.

3. Deitz, Larry. "Computer Security in the Micro Age." Computers & Electronics, Vol. 22, No. 6 (June 1984): pp. 68-70+.

4. Emmett, Arielle. "Thwarting the Data Thief." Personal Computing, Vol. 8, No. 1 (January 1984): pp. 98-99+.

Official Documents

5. U.S. Department of the Air Force. Air Force Privacy Act Program. AF Regulation 12-35. Washington, D.C.: Government Printing Office, 1983.

6. U.S. Department of the Air Force. Automatic Data Processing (ADP) Security Policy, Procedures, and Responsibilities. AF Regulation 205-16. Washington, D.C.: Government Printing Office, 1984.

7. U.S. Department of the Air Force. Automatic Data Processing Resource (ADPR) Management. AF Regulation 300-6. Washington, D.C.: Government Printing Office, 1980.

8. U.S. Department of the Air Force. Communications Security Policies, Procedures, and Instructions. AF Regulation 100-45. Volume I. Washington, D.C.: Government Printing Office, 1980. FOR OFFICIAL USE ONLY.

9. U.S. Department of the Air Force. Information Security Program. AF Regulation 205-1. Washington, D.C.: Government Printing Office, 1982.

10. U.S. Department of the Air Force. Management of Small Computers. AF Regulation 300-3. Washington, D.C.: Government Printing Office, 1984.

11. U.S. Department of the Air Force. The Resources Protection Program. AF Regulation 125-37. Washington, D.C.: Government Printing Office, 1982.

12. U.S. Department of the Air Force. Safeguarding Personal Data in Automatic Data Processing Systems. AF Regulation 300-13. Washington, D.C.: Government Printing Office, 1976.

13. U.S. Department of the Air Force. Standards of Conduct. AF Regulation 30-30, Washington, D.C.: Government Printing Office, 1983.

14. U.S. Department of the Air Force: Air Force Data Systems Design Center (DMT). Air Force Byte Line. Volume I. Number 1. Gunter Air Force Station, Alabama, no date.

15. U.S. Department of the Air Force: Air Force Data Systems Design Center (DMTD). A Small Computer Security Handbook. Gunter Air Force Station, Alabama, [1983].

16. U.S. Government: Office of Management and Budget. Security of Federal Automated Information Systems. OMB Circular No. A-71, Transmittal Memorandum No. 1. Washington, D.C., 27 July 1978.

Unpublished Materials

17. Doll, Richard D., Lt Col, USAF. "Small Computer Security." Lecture presented at the Air Command and Staff College, Maxwell Air Force Base, Alabama, 5 October 1984.

18. U.S. Department of the Air Force: Air Force Computer Security Program Office (CK). Handout for equipment ordered under Air Force Contract F19630-84-D-0009. Gunter Air Force Station, Alabama, no date.

19. U.S. Department of the Air Force: Air Force Information Systems Doctrine Office. Information Systems Security. AF Regulation 700-10 (draft). Keesler Air Force Base, Mississippi, no date.

20. U.S. Department of the Air Force: HQ United States Air Force (SI). "Copyrighted Software," message. Washington, D.C., 25 November 1983.

21. U.S. Department of the Air Force: HQ United States Air Force (SI). "Secure Microcomputer Environment," message. Washington, D.C., 28 June 1984.

22. U.S. Department of the Air Force: HQ United States Air Force (SI). "Security Procedures for TEMPEST Small Computers," message. Washington, D.C., 2 May 1984.

23. U.S. Department of the Air Force: HQ United States Air Force (XO-I). "OPSNET Prototype Workstation Security Plan." Washington, D.C., 20 August 1984.

24. U.S. Government: Department of Commerce (National Bureau of Standards). Security Considerations for Small Computer Systems: A Preliminary Guide for Managers and Users. NBS Special Publication 500- (draft). Washington, D.C., no date.

Other Sources

25. Southerland, Barbara K. Information Systems Security Specialist, Air Force Computer Security Program Office, Gunter Air Force Station, Alabama. Interview, 26 October 1984.

26. Trapp, Paul A. Deputy Program Manager for Policy and Procedure, Air Force Computer Security Program Office, Gunter Air Force Station, Alabama. Interview, 26 October 1984.

B. RELATED SOURCES

Official Documents

U.S. Department of the Air Force. Automated Data System Project Management. AF Regulation 300-15. Washington, D.C.: Government Printing Office, 1978.

U.S. Department of the Air Force. Communications-Electronics Terminology. AF Manual 11-1. Volume III. Washington, D.C.: Government Printing Office, 1973.

U.S. Department of the Air Force. Managing Air Force Information Systems. AF Regulation 700-1. Washington, D.C.: Government Printing Office, 1984.

U.S. Department of the Air Force. Managing the USAF Automated Data Processing Program. AF Regulation 300-2. Washington, D.C.: Government Printing Office, 1980.

U.S. Department of the Air Force. *Procedures for Managing Automated Data Processing Systems (ADPS).* AF Regulation 300-12. Volume I. Washington, D.C.: Government Printing Office, 1977.

U.S. Government: Department of State. *Security Standards for Office Automation Systems Used for National Security Information in the Washington, D.C. Metropolitan Area.* A/ISS Systems Security Standard Number 1. Washington, D.C., 22 December 1983.

Unpublished Materials

U.S. Department of the Air Force: Air Force Audit Agency. *Report of Audit: Review of Internal Controls for Small Computer Systems.* Project 3120115 (draft). Washington, D.C., no date.

U.S. Government: Department of Commerce (National Bureau of Standards). *Guide on Selecting ADP Backup Alternatives* (draft). Washington, D.C., no date.

APPENDIX A

SAMPLE DECLASSIFICATION LOG

Below is a sample declassification log. Be sure to maintain a log for each small computer system and all software and data media that will be declassified. In order to keep track of the media (floppy diskettes, hard disks, cartridges, ribbons, etc.), you will want to uniquely identify each item. Serial numbers are available for hard disks. For other media, consider a numbering system such as the owner's initials and sequence number (e.g., JBW-1, JBW-2, PHT-1, PHT-2).

DECLASSIFICATION LOG

ITEM: Zenith Z-150 system (serial number 3650244)
with peripherals

DATE	TIME	DECLASSIFIED BY	WITNESS

NOTE: Retain this document for two (2) years.

NO PRINT

APPENDIX B

SAMPLE MAINTENANCE LOG

Below is a sample maintenance log for a small computer system. It is a condensed version of AF Form 597. Use this log to keep track of all maintenance performed on all components of the system.

MAINTENANCE LOG

System: IBM PC, Model 5150, Serial Number 23642
with: IBM keyboard
IBM color board
64K RAM
two (2) DS/DD disk drives
AST SixPakPlus card [256K RAM], Serial Number 37482
PGS RGB color monitor, Serial Number 04832
Epson MX-80F/T printer, Serial Number 891243

ITEM	DATE	DESCRIPTION OF PROBLEM	DATE OF REPAIR	DESCRIPTION OF REPAIR	MAINTENANCE PERSONNEL NAME

NO PRINT

APPENDIX C

SAMPLE MEDIA CONTENTS LOG

The following is a sample log of the contents of a floppy diskette. Note that the log is simply a directory listing of the diskette along with a handwritten description of the files.

The log you generate can be as simple as this one.

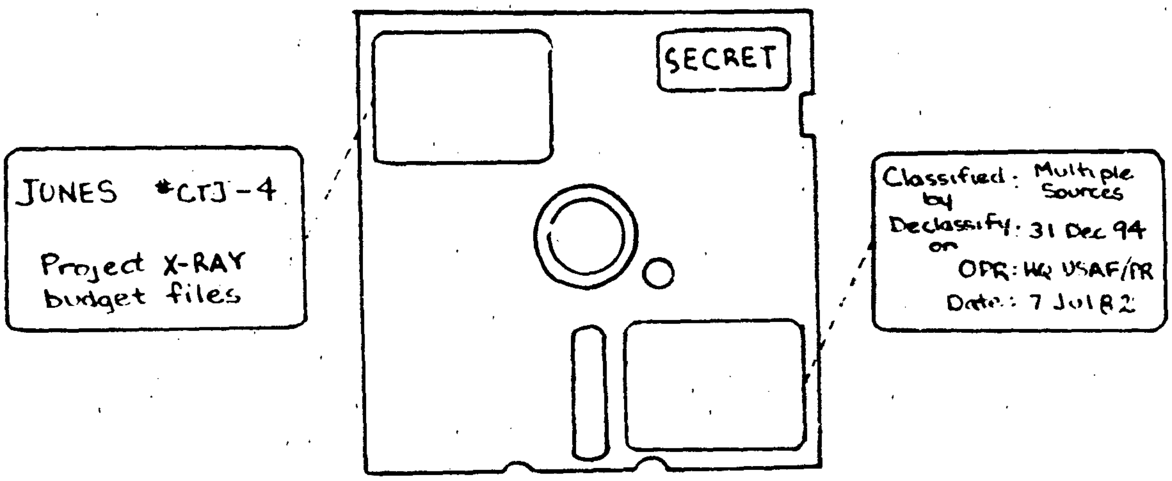
```
 Volume in drive A is HANDBOOK                      Diskette # JBW-1
 Directory of  A:\

CONTENTS          2816  12-11-84   6:20p — table of contents
PREFACE           2432  12-11-84   6:19p — preface
CHAPTER1          4608  12-11-84   6:21p — chapter 1
CHAPTER2          7936  12-11-84   6:39p — chapter 2
CHAPTER3         15872  12-11-84   6:40p — chapter 3
CHAPTER4         32128  12-11-84   7:18p — chapter 4
CHAPTER5         31872  12-11-84   7:30p — chapter 5
CHAPTER6          7552  12-11-84   5:56p — chapter 6
CHAPTER7          1152  12-11-84   6:06p — chapter 7
        9 File(s)    210944 bytes free
                                          NOTE: All files are WordStar files.
```

NO PRINT

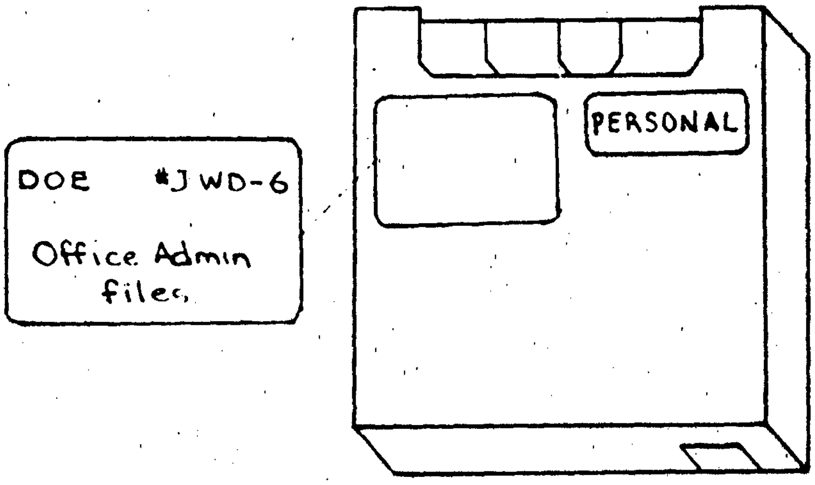
APPENDIX D

SAMPLE SENSITIVITY MARKINGS FOR MAGNETIC MEDIA

Below are two examples of sensitivity markings. One is for a floppy diskette; the other is for a cartridge.



floppy diskette



cartridge

NO PRINT

APPENDIX E

SAMPLE SOFTWARE INVENTORY

A sample software inventory is provided below. The first inventory should be conducted when the small computer first arrives. Be sure to update the inventory whenever new applications are added to the system and when updated versions of the software acquired. Remember application programs developed for the system should be inventoried as well as standard applications packages.

SOFTWARE INVENTORY

SYSTEM/ SERIAL NUMBER	NAME OF PACKAGE	VERSION	LICENSE NUMBER/ SERIAL NUMBER	NUMBER OF DISKETTES	DOCUMENTATION

NO PRINT

APPENDIX F

GENERAL PURPOSE SMALL COMPUTER SECURITY CHECKLIST

NOTE: An annotation preceding an item means that current rules require the action be taken for the categories as defined below:

A - all computer systems
S - systems processing sensitive or classified information
L - systems processing classified information
R - critical systems
T - TEMPEST systems

PLANNING PHASE:

A - 1. Conduct a risk analysis. Your primary responsibilities are as follows:

- determine the type of data your system will process (personal data, secret data, etc.)
- determine the sensitivity of the data
  (ADP-I: critical-sensitive
  ADP-II: noncritical-sensitive
  ADP-III: non-critical)
- determine the criticality of the system
  (ADP-I: highly-critical
  ADP-II: critical
  ADP-III: non-critical)
- select the appropriate security measures for the system

R - 2. Develop a contingency plan. You must:

- select an alternative for backing up the software and data
- develop an operations contingency plan to deal with losses in processing capability (i.e., theft of hardware, hardware failure, etc.)

(continued on the next page)

ONE-TIME MEASURES:

SR - 3. Check to ensure the DAA has approved the system for use

A - 4. Appoint a TASO

A - 5. Appoint an equipment custodian

A - 6. Add the computer system to the nightly security inspection checklist

A - 7. Establish a maintenance log

L - 8. Establish declassification logs

A - 9. Add the system to the ADPE inventory

10. Conduct a software inventory

R - 11. Back up all applications software packages. Remember to:

- have at least one backup copy of all applications programs
- make copies of the master software diskettes as the working copies of the applications programs
- treat software master diskettes as backup copies
- if software must be installed, have a backup copy of the installed version
- back up documentation as required (do NOT make illegal copies)

S - 12. Create a minimum of two "boot" diskettes to be used for unclassified and sensitive or classified processing, respectively

S - 13. Create a minimum of two sets of all applications software to be used for unclassified and sensitive or classified processing, respectively

S - 14. Establish procedures for keeping track of information stored on magnetic media

S - 15. Limit physical access to the system. Options include:

- new locks
- security alarms
- secure office area
- key control procedures

16. Location considerations:

T - - check with TEMPEST officer before locating the system
- locate to ensure adequate ventilation
- keep system away from sprinkler system

T - locate so video display and printer/plotter outputs cannot be seen
- keep away from vibrations

17. Set-up measures:

T -
- configure system with only TEMPEST equipment
- printers and plotters kept separately from main unit and hard disks
- ground system properly
- do NOT use extension cords
- do NOT use 3-prong to 2-prong converters
- use surge protectors
- connect components to a high quality power strip
- do NOT put "electricity hungry" appliances (coffee pots, space heaters, vacuum cleaners, etc.) on the same circuit as the small computer system

18. If static electricity is a problem:

- use ground floor matts
- use humidifier

19. If air quality is poor, use air cleaner

20. If electricity quality is poor, get new circuit

(continued on the next page)

RECURRING PROCEDURES:

21. Do NOT eat, drink, or smoke around the system

22. Do NOT bump into the system

23. If static electricity is a problem:

- use static electricity sprays
- ground yourself before you touch the system

24. Clean system components regularly (if TEMPEST system cannot open system w/out compromising TEMPEST integrity)

25. Do NOT operate system during thunderstorms

A - 26. Do NOT misuse your system, i.e. hardware, software, supplies, and computer time

SR - 27. Do NOT use personally owned small computers

28. If there is a fire:

- turn off the system
- do NOT use water
- avoid CO2 if possible (do NOT use CO2 until video display is turned off)
- use Halon when available

A - 29. Update the ADPE inventory as required

A - 30. Maintain the system maintenance log

31. Maintain a current software inventory

32. Do NOT modify standard, off-the-shelf software

33. Do NOT indiscriminately modify applications programs developed for your system

A - 34. Do NOT illegally duplicate software or its documentation

R - 35. Back up your data on a routine basis

- copy, as a minimum, all data having changed since the last backup
- store media in a safe place

36. Write-protect files when utility is available

S - 37. Keep track of information stored on magnetic media

38. Handling magnetic media:

- do NOT touch exposed surfaces
- use only felt tip pen to write on labels
- avoid exposure to magnetic fields
  -- keep at least one foot away from appliances
  -- do NOT lay next to or on top of video displays
- for floppy diskettes:
  -- do NOT take out of its jacket
  -- do NOT bend
  -- store vertically
- for hard disks:
  -- avoid vibrations

S - 39. Control access to the system. This requires you to:

- monitor who has access to the computer work area
- allow only authorized maintenance on the system. This means you must:
  -- allow authorized personnel only
  -- verify security clearance of personnel perfomring maintenance
  -- maintain maintenance log

S - 40. Control access to data. This requires you to:

L - - operate in dedicated security mode
L - -- limit system access to users who have the security clearance and need-to-know for all data residing on the system
S - -- system sensitivity level established as sensitivity level of the most sensitive data it is processing, using, storing, or producing
S - -- treat all data output, including floppy diskettes, cartridges, hard disks, printer/plotter ribbons, and computer output hardcopies, at the sensitivity level of the system until the data is individually reviewed to assess its sensitivity
L - - declassify system when:
-- maintenance to be performed
-- moving system to another location
L - - if not in controlled area, declassify system when:
-- changing sensitivity level to lower level
-- going from classified to unclassified processing
-- leaving system unattended
S - - treat media like sensitive documents
-- AFR 205-1 applies to all classified media
-- AFR 12-35 applies to all Privacy Act data
-- "treatment" includes access, marking, storing, viewing, transferring, and declassifying
S - - use appropriate diskette to "boot" the system
S - - use appropriate set of software media to operate the system
L - - share media among users of if users have both the security clearance and the need-to-know for all the data stored on the media

S - 41. Mark the sensitivity of the software or data residing on the magnetic media:

- AFR 205-1 applies
- label designating highest level of data or software recorded on it since media was last declassified
- label designating classification source, downgrading instructions, etc. as required by AFR 205-1
- label identifying ownership and general contents

L - 42. Declassify the system when required:

- remove and safeguard all sensitive media (magnetic media, printer/plotter ribbons, and computer hardcopy)
- turn the video display control to its maximum brightness. Turn off all system components except the video display. Wait five seconds. Turn off the video display.
- Log the declassification on the declassification log.
  NOTE: If you plan to use the system again, wait ten seconds before turning the system back on.

L - 43. To declassify magnetic media:

- method 1 (for floppy diskette):
  -- use tape degausser on floppy diskette
  -- log the declassification

or - method 2 (for floppy diskette):
  -- reformat the diskette
  -- copy the entire contents of an unclassified, non-sensitive diskette onto the diskette being declassified
  NOTE: If a "DISKCOPY" or like command is used, the diskette being declassified does not have to be reformatted before the copy procedure begins.
  -- repeat the above two steps two more times
  -- compare the contents of the two diskettes
  -- change the sensitivity markings on the diskette
  -- log the declassification
- use method 1 or 2 above for other magnetic media

NOTE: Do NOT use degaussers on hard disks.

L - 44. To declassify printer/plotter ribbons:

- film ribbons can NOT be declassified
- for ribbons that can be overwritten:
  -- overwrite with unclassified, non-sensitive data consecutively five times
  -- change the sensitivity markings on the ribbon
  -- log the declassification

L - 45. To declassify computer printouts follow the procedures as defined in AFR 205-1

A - 46. To destroy all software and data media:

- if the software or data is unclassified, the media will be burned
- if the software or data is classified, the media will be destroyed according to the standard destruction procedures for classified data

47. General operating instructions:

L - - determine if and when system declassification is required

- to begin processing:

A - -- determine sensitivity level of the system

S - -- if processing sensitive data, disconnect the system from any communications links

-- insert appropriate ribbon(s) into the printer and plotter

S - -- "boot" the system using the appropriate boot diskette

- during processing:

S - -- use the data media you need for processing at the sensitivity level you determined

S - -- maintain access control to your system and your data

T - -- maintain TEMPEST integrity by following procedures for operating the hardware on your TEMPEST system (i.e. close doors, lower printer lids, etc.)

S - -- monitor output to all data media and safeguard the media at the sensitivity level of the system until the actual sensitivity level of the data has been determined

- to end processing:

S - -- remove and safeguard all data media

L - -- declassify the system if required

-- turn the system off

NO PRINT

INDEX

END

FILMED

9-85

DTIC